INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

REVIEW ON MOBILE APPLICATION IN A CLOUD COMPUTING SECURE AND SCALABLE USING CLOUD HOSTED KEY

MR. SUNNY W. THAKARE, MR. N. R. CHOPDE

Department of C.S.E, M.E (G. H. Raisoni. C. E & M. Amravati)

Accepted Date: 05/03/2015; Published Date: 01/05/2015

Abstract: Mobile cloud computing is a model for transparent elastic augmentation of mobile device capabilities via ubiquitous wireless access to cloud storage and computing resources, with respect to change in operating conditions." The foundation of cloud computing is the delivery of services, software and processing capacity over the Internet, reducing cost, increasing storage, automating systems, and providing flexibility and mobility of information. User data may be stored in a cloud to take advantage of its scalability, accessibility, and economics. However, data of a sensitive nature must be protected from being read in the clear by an untrusted cloud provider. It is also beneficial to provide finite time limits on access to the data by users. A key management scheme is proposed where encrypted key shares are stored in the cloud and automatically deleted based on passage of time or user activity. The accessibility of the data gradually expires and revocation occurs as a result of the loss of sufficient key shares. Subscription to user data is maintained through regular re-generation of shares. For better understand of mobile cloud-based applications, I have surveyed existing work in mobile computing through the prism of cloud computing principles.

Keywords: Cloud computing; mobile computing, Distributed systems, security, cryptography.

Corresponding Author: MR. SUNNY W. THAKARE

Access Online On:

www.ijpret.com

How to Cite This Article:

Sunny W. Thakare, IJPRET, 2015; Volume 3 (9): 92-99

PAPER-QR CODE

INTRODUCTION

Cloud computing systems offer nearly unbounded storage and computation for clients. In many applications, however, the provider of cloud services cannot be sufficiently trustworthy to permit storing and processing of data. Cloud applications are accessed by potentially thousands of mobile device users, an encrypted cloud storage solution requires scalable key management.

Current key management typically focuses on key generation and distribution among a large population of users. The primary concern is that as authorized users join and leave a system, current keys must be re-generated and re-distributed to valid users, which is an unrealistic cost for mobile device users. [1] The key design factors for a cloud-based secure storage system include: server-side logic being required on the cloud provider end; fine-grained data access; highly scalable sharing among multiple readers and writers; having unrestricted access to stored user data. The combination of cloud computing, wireless communication infrastructure, portable computing devices, location-based services, mobile Web, etc., has laid the foundation for a novel computing model, called mobile cloud computing, which allows users an online access to unlimited computing power and storage space.

OVERVIEW OF MCC

The term “**mobile cloud computing**” was introduced concept of “cloud computing” launched in mid-2007? It has been attracting the attentions of entrepreneurs as a profitable business option that reduces the development and running cost of mobile applications, with low cost. [3]

A. What is Mobile Cloud Computing?

“Mobile Cloud Computing (MCC) is a simplest infrastructure where both the data storage and the data processing happen outside of the mobile device.”

Mobile Cloud:

The mobile cloud is an instance of technology using cloud computing in mobile environment. It is based on a collection of many old and few new concepts in several research fields like Service-Oriented Architecture (SOA), distributed and grid computing over the network. The key opinion expressed by the cloud computing is to transfer the complex computing to the cloud and the service-oriented concept. So I proposed the mobile cloud to solve this constraint. With mobile cloud, users just need to send their requests for certain service and the cloud provides the service. The mobile host does not need to pay much computing time for complex services.

The mobile cloud consists of two kinds of cloud units: cloud units in every cell region and remote cloud units. & divided into five layers See Figure 1 are as:-

- Cloud Application Layer
- Cloud Software Environment Layer
- Cloud Software Infrastructure Layer
- Software Kernel
- Hardware and Firmware

DELIVERY MODELS OF CLOUD COMPUTING

Once an Internet connection is established among several computers, it is possible to share services within anyone of the following service models.

A. Cloud Software as a service (SaaS)

The capability provided to the consumer is to use the provider's application running on a cloud infrastructure. &client interface such as a web browser. [2].

Advantages: Rapid start-up, maintenance and upgrades performed by the vendor.

Risks: Minimal customization, data integration, security.

Examples: Salesforce.com, Google Apps.

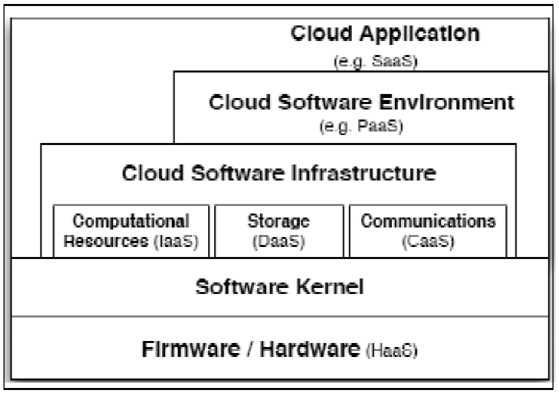
Cloud Application
(e.g. SaaS)
Cloud Software Environment
(e.g. PaaS)
Cloud Software Infrastructure
Computational Resources (IaaS)
Storage (DaaS)
Communications (CaaS)
Software Kernel
Firmware / Hardware (HaaS)

Figure 1: Architecture of Model

B. Cloud Platform as a service (PaaS)

It include complete application hosting, development, testing and deployment environment.

Advantages: Focus on high value rather than infrastructure.

Risks: Exit strategy, pricing model, upgrade issues. Examples: force.com, web and e-mail hosting.

C. Cloud Infrastructure as a Service (IaaS)

It is able to deploy and run arbitrary software, which can include operating system and application.

Advantages: Scalable, rapid start-up, peak leveling.

Risks: Pricing model, potential lock-in, security and privacy, proliferation Examples: Amazon EC2, Rackspace.

DEPLOYMENT MODELS

A. Public Cloud

Public cloud or external cloud describes cloud computing in the traditional main stream sense, see Figure. 2 whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet. [3].

B. Community cloud

Several organizations have similar requirements and share infrastructure of cloud computing. But it may offer a higher level of privacy, security. Examples Google's "Gov. Cloud".

C. Hybrid cloud

The term "Hybrid Cloud" has been two separate clouds (public, private, internal or external). "Hybrid Cloud" is probably the use of physical hardware and virtualized cloud server [2]. An deploying a web application in the cloud is using Hybrid Web Hosting, where the hosting infrastructure is a mix between Cloud Hosting and Managed dedicated servers –as part of a web cluster. It uses both public and private storage clouds. It archiving and backup functions as local data in a public cloud.

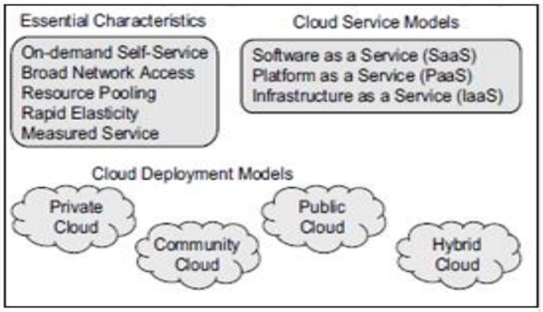

Figure 2: Cloud Model

D. Private Cloud

Cloud computing on private networks offer ability to host applications. Generally private clouds are hosted by third parties, rather than being hosted on dedicated servers. User store large data to hosted companies.

RELATED REVIEW WORK

Various access control techniques have been proposed for encrypted file storage in the cloud. The cloud provider typically controls key management activities, or the data owner or a trusted proxy requiring additional network communication and components [2]. In some mechanisms where control rests within the domain of the client, such as cloud-based data re-encryption [3]. The scalable storage been under-utilized for key management operations. NIST (National Institute of Standards and Technology) [4] recommends secret sharing as a technique to be used to protect long-term credentials in its level 3 security definition for a CSP (Cloud Service Provider). Secret key sharing allows a secret such as key information to be divided into multiple shares [1]. These shares may be distributed among key generators using the concept of threshold decryption [4], or portions of a private key are distributed among users [4]. The challenge is that the client must assemble a key from multiple sources. & key shares being distributed on demand by some authority with distributed across a network for some time.

The Vanish system [2] distributes shares onto a DHT (Distributed Hash Table) that underlies a peer-to-peer file sharing network. It suggests the concept of “self-destructing data,” where copies of data become unreadable over time due to the effect of user churn on the index. It requires that each user obtain key shares from multiple other nodes that form the index, if the user is operating a mobile device.

In the DEPSKY [5] storage system, shares are necessarily distributed across multiple clouds to form distributed trust and to restrict access. Each cloud provider has access to a single share and thus cannot decode the stored data; this requires support for a cloud-of-clouds. Also, because the data shares are unencrypted, each cloud must be independent and collusion assumed to be impossible.

A straightforward approach employing PGP encryption [3] would encounter challenges with scalability for instance. The symmetric key used for encryption of user data may need to be encoded with the public key of each recipient. & it is preferable for a one-time encryption. If the same private key is shared by all users, then revocation would require some form of authentication to trust provider.[6]

System and Threat Models

In this model self-eroding key material in the cloud is achieve highly scalable access management for mobile users. Models are as:-

A. System model

Consider a large population of mobile device users that accesses data in the cloud having communication sessions with wireless transmission. Users are expected to only communicate directly with the cloud. Communication between users and the cloud takes place over an insecure wireless medium subject to the risk of eavesdropping with secure communication. The permanent cloud data store is accessed through a key value mechanism, in which a valid key index must be supplied to retrieve the value stored at the index location.

B. Threat model

The cloud provider is assumed to be an untrusted entity. It provides reliable service to users for storage capacity on demand. The mobile device users all belong to the same organization and can freely share information. Once a user’s access any valid key information in the cloud may continue to provide access to encrypted user data. Computer security are required to ensure that secret information between a mobile user and an outside attacker.

PROPOSED MODULE

The following Secret Shamir & RC6 algorithm is used to access the encrypted data in the cloud through the process of storing and removing encrypted key shares in the cloud. For some techniques use as: [2]

A. Main technique

1) Key generation and encryption

2) Metadata

3) Decryption

4) Key share deletion

5) Key share replacement

6) Revocation

B. Analysis

The main use of manage Key to shares &stored data securely in the cloud. For authorized user, with a unique access key.

C. Trust, Security and Privacy

A never ending issue will always be security provide through my project algorithm [4].

CONCLUSION

Finally, I have conclude that all several approaches being overview of wide spectrum of mobile cloud computing. None of the existing approaches meets in my project. Native (offline) and Web (online) applications are the two extremes of mobile applications. Using Mobile cloud computing will solve the problems in information and communication technology in secure and scalable region over the cloud with the help of scalable keys.

REFERENCE

1. Piotr K. Tysowski, M. Anwarul Hasan, Cloud-Hosted Key Sharing Towards Secure and Scalable Mobile Applications in Clouds, International Conference on Computing, Networking and Communications 978-1-4673-5288-8/13/$31.00 ©2013 IEEE Vol 1(Sep-2013)

2. Hoang T. Dinh, Chonho Lee, Dusit Niyato, and Ping Wang, IEEE A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches (Dec-2011)

3. CSA, "Security Guidance for Critical Areas of Focus in Cloud Computing," V2.1, http://www.cloudsecurityalliance.org/guidance/csaguide.pdf

4. P. Tysowski and M. A. Hasan, “Towards Secure Communication for Highly Scalable Mobile Applications in Cloud Computing Systems,” Centre for Applied Cryptographic Research, University of Waterloo, Tech. Rep. CACR 2011-33, 2011.

5. Kamal Dahbur, Bassil Mohammad, Ahmad Bisher Tarakji, A Survey of Risks, Threats and Vulnerabilitiesin Cloud Computing, International Journal of Emerging trends in Engineering and Development ISSN 7899-6436 Issue1, Vol. 3(Aug-2011)

6. Itani W, Kayssi A, and Chehab A. Privacy as a service: Privacy- aware data storage and processing in cloud computing architectures. In: Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC09). Chengdu, China, 2009: 711-716.